

DESAIN DAN IMPLEMENTASI SISTEM TELEMEDICINE UNTUK PERIKSA KESEHATAN MANDIRI MENGGUNAKAN QR CODE AUTHENTICATION BERBASISKAN ANDROID

DESIGN AND IMPLEMENTATION OF TELEMEDICINE SYSTEM FOR SELF CHECKUP USING QR CODE AUTHENTICATION BASED ON ANDROID

Dhea Dearly Herman¹, Favian Dewanta, Ph.D.², Sussi, S,Si., M.T.³

^{1,2,3}Prodi S1 Teknik Telekomunikasi Fakultas Teknik Elektro, Universitas Telkom

¹dheadearly@student.telkomuniversity.ac.id, ²favian@telkomuniversity.ac.id,

³sussiss@telkomuniversity.ac.id

Abstrak

Dalam mencegah penyebaran virus COVID-19, pasien dianjurkan untuk tidak pergi ke fasilitas kesehatan kecuali dalam keadaan yang darurat. Pengaplikasian sistem telemedicine untuk diagnosis dan monitoring kesehatan dari jarak jauh sangat dibutuhkan. Maka dari itu Tugas Akhir berpusat pada desain dan implementasi sistem telemedicine untuk periksa kesehatan mandiri dengan menggunakan aplikasi android "Self Checkup". Sistem ini dirancang menggunakan framework React Native untuk memeriksa kesehatan pengguna dengan melihat data secara realtime dari tiga IoT healthcare device yaitu Weight Scale Device, Body Temperature Device, dan IoT Healthcare Device melalui NodeMCU ESP32 dengan protokol komunikasi Bluetooth Low Energy. Pairing antara aplikasi android dengan IoT device menggunakan metode otentikasi dengan QR Code. Kemudian data yang diterima dari IoT device dienkripsi dengan algoritma AES 256-bit lalu dikirimkan ke cloud server. Hasil pengujian Quality of Service dari ketiga IoT healthcare device ke aplikasi android memperoleh nilai rata-rata delay sebesar 97 ms, throughput sebesar 2.424 Kbps dan packet loss sebesar 0%. Nilai rata-rata delay dari aplikasi android ke cloud server sebesar 203 ms, throughput sebesar 4.624 Kbps dan packet loss sebesar 0%. Hasil pengujian performansi algoritma AES 256-bit memiliki rata-rata waktu enkripsi sebesar 54 ms dan dekripsi sebesar 72 ms.

Kata kunci : Aplikasi Android, QR Code, Internet of Things, Bluetooth Low Energy, Telemedicine, Cloud Server, AES.

Abstract

In preventing the spread of COVID-19, patients are advised not to go to health facilities except in an emergency. Telemedicine system application for remote health diagnosis and monitoring is urgently needed. Therefore, the final project focuses on the design and implementation of the telemedicine system for independent health checks using the android application "Self Checkup". This system was designed using the framework React Native to check the user's health by looking at the data in real-time from three IoT healthcare devices, which are Weight Scale Device, Body Temperature Device, and electrocardiogram device through NodeMCU ESP32 with Bluetooth Low Energy communication protocol. Pairing between the android application and the IoT device is conducted by using an authentication method based on QR code. Then the data received from the IoT device are encrypted with a 256-bit AES algorithm before being sent to the cloud server. The quality of service (QoS) experiments from the three IoT healthcare devices to the Android applications show that the average delay value is 97 ms, throughput is 2.424 Kbps and packet loss is 0%. Meanwhile, the QoS experiments between the Android application and cloud server show that the average delay is 203 ms, throughput is 4.624 Kbps and packet loss is 0%. As for the security performance of the 256-bit AES algorithm, the average encryption is 54 ms and AES decryption is 72 ms.

Keywords: Android Application, QR Code, Internet of Things, Bluetooth Low Energy, Telemedicine, Cloud Server, AES.

1. Pendahuluan

Pandemi COVID-19 mengubah aspek kehidupan seluruh masyarakat dunia di berbagai bidang dan memengaruhi masa yang akan datang[1]. Dalam beberapa tahun terakhir, perkembangan teknologi informasi sudah banyak menyediakan layanan yang memenuhi kebutuhan sehari-hari. Dengan adanya kebijakan pemerintah agar tetap berada di rumah dan jaga jarak memberi dampak terhadap interaksi antar sesama menjadi lebih virtual. Menurut OpenVault Broadband Insights Report pada kuartal pertama tahun 2020 penggunaan internet broadband meningkat 47 persen[2]. Untuk mencegah penyebaran virus, pasien dianjurkan untuk tidak pergi ke fasilitas kesehatan kecuali dalam keadaan yang darurat. Pengaplikasian sistem telemedicine untuk diagnosis dan monitoring kesehatan dari jarak jauh pada kondisi pandemi sangat dibutuhkan. Telemedicine merupakan layanan kesehatan agar pasien dapat berkonsultasi dengan dokter jarak jauh tanpa harus bertemu dan kemungkinan besar menjadi bagian umum dari praktik medis di masa depan[3].

Sebelum pandemi juga sudah banyak implementasi mengenai telemedicine seperti layanan berbicara langsung dengan dokter. Kemudian sudah banyak aplikasi untuk mengawasi kondisi kesehatan tubuh juga sudah banyak di internet, seperti Reminder, Health, Fitness, Diet, dan lain-lain yang dimana data kesehatan tubuh di input ke dalam aplikasi. Namun terdapat kekurangan yaitu dokter tidak bisa mendiagnosis pasien dengan akurat karena tidak melakukan pemeriksaan kesehatan secara langsung melainkan dari yang dikirim dari pasien yang belum tentu akurat[4]. Keluaran dari aplikasi ataupun diagnosa dokter tersebut bisa sama dengan kebenaran dan berbeda tergantung dari pengguna memasukkan data. Maka dari itu untuk pemeriksaan kondisi kesehatan jarak jauh dibutuhkan peralatan medis yang terintegrasi dengan sistem telemedicine agar dokter dapat menganalisa sesuai dengan keluaran alat[5].

Tugas akhir berpusat pada perancangan dan implementasi sistem telemedicine berupa aplikasi android "Self Check Up" bertujuan untuk periksa kesehatan secara mandiri yang terhubung dengan tiga IoT Healthcare Device, yaitu Weight Device yang memiliki sensor berat badan Load Cell, Temperature Device yang memiliki sensor suhu tubuh MLX90614, dan ECG Device yang memiliki sensor sinyal detak jantung ECG AD8232 melalui NodeMCU ESP32 dengan protokol komunikasi Bluetooth Low Energy. Pairing antara ketiga IoT Device dengan Aplikasi Android menggunakan metode otentikasi QR code. Ketika pengguna menggunakan device, aplikasi android akan menampilkan data kesehatan secara real-time dan sistem mengirimkan data kesehatan pengguna ke MongoDB database melalui Cloud server. Diharapkan dengan adanya sistem yang dibuat, pengguna bisa memeriksa kesehatan secara mandiri dirumah saja setiap harinya. Tenaga kerja medis bisa mengakses data perkembangan kesehatan melalui database.

2. Perancangan Sistem

2.1 Tinjauan Pustaka

2.1.1 Telemedicine

Telemedicine secara harfiah berarti penyembuhan dari jarak jauh dengan memanfaatkan teknologi informasi dan komunikasi dengan memudahkan akses ke tenaga kerja medis. Tujuannya adalah memberikan dukungan klinis, mengatasi hambatan geografis dengan menghubungkan pengguna yang tidak berada di lokasi fisik yang sama dan meningkatkan hasil kesehatan bagi pasien[6].

2.1.2 Internet of Things (IoT)

IoT merupakan konsep dari pengembangan teknologi yaitu internet tidak hanya menghubungkan antar manusia tetapi menghubungkan semua benda dan perangkat yang ada menggunakan sensor yang terdapat dalam setiap perangkat fisik sehari-hari. Sensor tersebut mengirimkan data dari perangkat menuju IoT platform yang mengintegrasikan data dari berbagai sumber untuk analisis lebih lanjut sesuai kebutuhan. IoT dapat memberi manfaat yang besar dalam bidang kesehatan yaitu dengan melihat perkembangan kesehatan pasien. Walau pasien berada di jarak yang jauh, data kesehatan mereka bisa dikirim ke dokter melalui IoT platform[7].

2.1.3 Medical Checkup

Dalam medical checkup atau pemeriksaan kesehatan secara menyeluruh, tenaga kerja medis akan memulai pemeriksaan fisik dengan mengukur kondisi tubuh seperti berat badan, suhu tubuh dan sinyal detak jantung terlebih dahulu disertai dengan pemeriksaan lain. Melalui medical checkup diharapkan suatu penyakit dan gangguan kesehatan dapat terdeteksi lebih awal. Pemeriksaan juga

menghasilkan metode penanganan dan pengobatan yang tepat sebelum penyakit berkembang[8]. Adapun data kesehatan untuk pemeriksaan kesehatan mandiri yang dirancang pada Tugas Akhir ini antara lain :

- a. Berat Badan
- b. Suhu Tubuh
- c. Detak Jantung

2.1.4 React Native

React Native merupakan framework untuk membuat aplikasi mobile bersifat open source yg dibuat oleh Facebook, Inc. React Native menggunakan bahasa Javascript bersifat hybrid karena kode program dapat langsung diimplementasikan pada Android dan iOS[9].

2.1.5 Android

Android merupakan sistem operasi berbasis Linux untuk mobile device seperti smartphone dan tablet yang bersifat open source dengan Lisensi Apache. Android menyediakan akses ke berbagai libraries dan tools yang dapat digunakan untuk membangun aplikasi. Android memungkinkan perangkat untuk berkomunikasi satu sama lain peer-to-peer. Selain itu, Android menggunakan mesin virtual khusus yang dirancang untuk mengoptimalkan memori dan sumber daya perangkat keras dalam mobile environment[10].

2.1.6 Bluetooth Low Energy

Bluetooth Low Energy (BLE) merupakan teknologi wireless personal area network hasil perkembangan dari Bluetooth classic yang ditujukan untuk protokol komunikasi IoT, Healthcare, Smart Home, dll. Sesuai namanya, BLE dapat menghemat daya dengan tetap berada pada mode sleep hingga terjadi inisiasi koneksi untuk komunikasi. Kecepatan pengiriman data BLE mampu mencapai 1 Mbit/s [11]. Koneksi pada BLE melibatkan dua peran terpisah yaitu Central/Master dan Peripherals/Slave. Central device biasanya ponsel atau PC yang memiliki daya pemrosesan CPU lebih tinggi. Central device berulang kali memindai frekuensi tertentu. Jika menemukan paket yang cocok, central device akan memulai koneksi. Setelah koneksi dibuat, central device mengatur waktu dan memulai pertukaran data. Peripheral device biasanya berupa beberapa sensor atau low power device, yang terhubung ke perangkat pusat. Jadi peripheral device mengirimkan paket secara berkala. Dan juga menerima koneksi masuk. Setelah dalam koneksi aktif, peripheral device mengikuti waktu pusat dan bertukar data secara regular[12].

2.1.7 QR Code

QR Code disingkat dari Quick Response Code adalah jenis barcode matriks (atau barcode dua dimensi) yang pertama kali dirancang pada tahun 1994 untuk industri otomotif di Jepang. QR code mudah dipindai oleh kamera smartphone, dimana saat QR code di scan oleh smartphone maka smartphone dengan cepat menampilkan informasi dari QR Code [13]. QR Code memiliki kelebihan daripada Barcode yaitu kapasitas data yang dalam kode, optimalisasi ukuran, dan bisa mengandung sebuah gambar. Hal-hal tersebut membuat QR Code banyak digunakan saat ini untuk pengkodean informasi bahkan untuk pembayaran digital [14].

2.1.8 Advanced Encryprion Standard

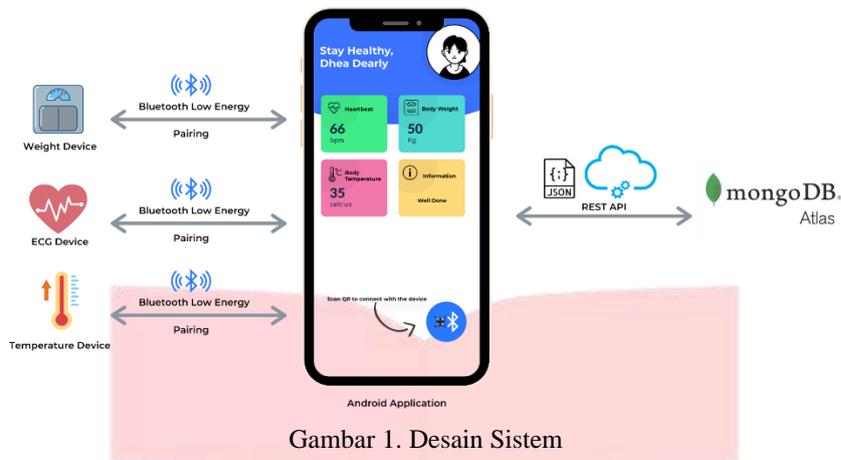
Advanced Encryption Standard (AES) merupakan algoritma kriptografi untuk mengamankan data oleh Vincent Rijmen dan John Daemen (Rijndael) yang merupakan lanjutan dari algoritma DES (Data Encryption Standar). AES adalah blok chipertext simetrik yang dapat mengenkripsi dan deskripsi informasi menggunakan kunci kriptografi 128, 192, dan 256 bit [15]. Dalam pengerjaan Tugas Akhir digunakan mode Cipher Block Chaining (CBC) dengan panjang kunci 256 bit dengan algoritma encode base64 sebagai format data ke cloud server, karena hasil dari encode base64 berupa text, lebih mudah dikirim dibandingkan dengan format data binary.

2.1.9 REST API

API adalah Application Program Interface merupakan kumpulan prosedur, fungsi, cara berkomunikasi atau peralatan untuk membuat software. Atau metode yang digunakan untuk komunikasi antar komponen dalam software. Digunakan dalam Web, Sistem Operasi, Database, Software dan Hardware. Teknologi untuk buat API diantaranya REST API yaitu Representational State Transfer (mekanisme API menggunakan HTTP atau Web sebagai protokol komunikasi. REST

bersifat bebas, rata-rata menggunakan JSON, sederhana, mudah dimengerti manusia, dan ringan. Pada Tugas Akhir untuk koneksi antara aplikasi android dengan cloud server menggunakan REST API.

2.2 Desain Sistem



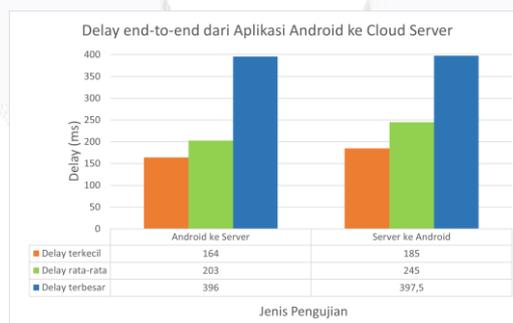
Gambar 1. Desain Sistem

Sistem telemedicine pemeriksaan kesehatan pribadi di rancang untuk mempermudah proses pengamatan mengenai suhu, detak jantung dan berat badan pengguna. Konsep dari sistem yang dibuat agar petugas medis dapat mengamati keadaan pasien dari tempat yang jauh dan tidak perlu bertatap langsung dengan pengguna sehingga memudahkan pengguna dalam menerima diagnosis awal dari data pemeriksaan dari sensor pada IoT Healthcare Device. Gambar 1 menjelaskan terdapat tiga input yaitu IoT Healthcare Device terdiri dari Weight Device, ECG Device dan Temperature Device melakukan komunikasi dengan Aplikasi Android dengan protokol komunikasi Bluetooth Low Energy (BLE). Saat pengguna menggunakan IoT Healthcare Device, data kesehatan akan muncul pada layar dan terintegrasi dengan MongoDB melalui Cloud server dan dapat dilakukan pengecekan kesehatan setiap harinya.

3. Hasil dan Analisis

3.1. Hasil Pengujian Performansi Jaringan dengan Quality of Service

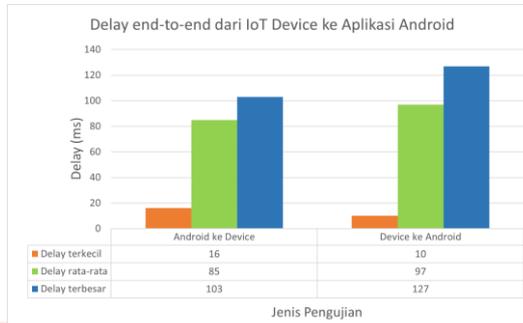
3.1.1 Delay



Gambar 2. Delay end-to-end dari Android ke Server

Pengujian delay skenario pertama menggunakan software Wireshark memfilter paket data dari IP Android dan IP Cloud Server. Jumlah pengujian pengiriman dan pengambilan data ke cloud server dilakukan sebanyak 30 kali. Gambar 2 menunjukkan bahwa delay dari aplikasi android menuju cloud server menggunakan metode POST memiliki nilai delay terkecil, delay rata-rata dan delay terbesar secara berurutan yaitu 164 ms, 203 ms dan 396 ms. Sedangkan untuk delay dari cloud server menuju aplikasi android menggunakan metode GET memiliki delay terkecil, delay rata-rata dan nilai terbesar secara berurutan yaitu 185 ms, 245 ms, dan 397, 5 ms. Terlihat dari dua jenis pengujian memiliki perbedaan tapi tidak terlalu jauh. Hal ini dipengaruhi oleh waktu pengujian delay pada waktu yang sama yaitu di malam hari selama 10 menit dari pukul 20.10 WIB sampai dengan 20.20 WIB. Kemudian untuk besar delay juga dipengaruhi oleh kinerja protokol HTTP yang memerlukan waktu untuk proses request dan response antara client dan server. Hasil delay rata-rata

dari android ke server ataupun server ke android sebesar 203 dan 245 ms sudah bisa dikatakan cukup baik karena waktu pengujian di malam hari yang merupakan jam sibuk atau penuhnya lalu lintas data penggunaan jaringan internet (overload traffic).



Gambar 3. Delay end-to-end dari Android ke Device

Pengujian delay untuk skenario kedua dengan mengaktifkan log Bluetooth Host Control Intervice di pengaturan Opsi Pengembang pada Aplikasi Android untuk mengetahui aktifitas dan hubungan bluetooth pada perangkat. Kemudian untuk menampilkan paket data menggunakan software Wireshark dengan cara open Bluetooth HCI Snoop Log. Pengujian delay dilakukan pengiriman dan pengambilan data ke IoT Healthcare Device sebanyak 30 kali. Gambar 3 menunjukkan bahwa delay dari aplikasi android menuju IoT Healthcare Device menggunakan metode WRITE memiliki nilai delay terkecil, delay rata-rata dan delay terbesar secara berurutan yaitu 16 ms, 85 ms dan 103 ms. Sedangkan untuk delay dari IoT Healthcare Device menuju aplikasi android menggunakan metode NOTIFICATION memiliki delay terkecil, delay rata-rata dan nilai terbesar secara berurutan yaitu 10 ms, 97 ms, dan 127 ms. Terlihat dari dua jenis pengujian tidak memiliki perbedaan yang signifikan. Semakin kecil nilai delay maka semakin baik performansi dari sistem. Untuk delay dari IoT Healthcare Device ke Aplikasi Android bisa dikatakan sangat bagus dimana kedua nilai tersebut dibawah 100 ms.

3.1.2 Packet Loss

Tabel 1. Packet Loss

No	Jenis Percobaan	Packet Loss
1	Android ke Server	0%
2	Server ke Android	0%
3	Android ke Device	0%
4	Device ke Android	0%

Berdasarkan Tabel 1. dapat dilihat bahwa rata-rata packet loss dari seluruh jenis percobaan Aplikasi Android dari/ke Cloud Server dan Aplikasi Android dari/ke IoT Healthcare Device sebesar 0% hal ini bisa dikatakan bahwa performansi jaringan dalam pengiriman paket data sangat baik.

3.2. Hasil Pengujian Performansi Keamanan dari Aplikasi Android

3.2.1 Lalu Lintas Data

```

00e0  6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 nnection : Keep-A
00f0  6c 69 76 65 0d 0a 41 63 63 65 70 74 2d 45 6e 63 live..Ac cept-Enc
0100  6f 64 69 6e 67 3a 20 67 7a 69 70 0d 0a 55 73 65 oding: g zip..Use
0110  72 2d 41 67 65 6e 74 3a 20 6f 6b 68 74 74 70 2f r-Agent: okhttp/
0120  33 2e 31 32 2e 31 32 0d 0a 0d 0a 7b 22 48 65 61 3.12.12...{"Hea
0130  72 74 5f 52 61 74 65 22 3a 22 38 30 20 62 70 6d rt_Rate" : "80 bpm
0140  22 7d }
    
```

Gambar 4. Lalu Lintas Data Sebelum Enkripsi

```

0120  33 2e 31 32 2e 31 32 0d 0a 0d 0a 7b 22 48 65 61 3.12.12...{"Hea
0130  72 74 5f 52 61 74 65 22 3a 22 35 68 4f 44 44 42 rt_Rate" : "5h00DB
0140  48 6f 34 64 70 4d 43 70 56 6b 6d 4d 51 70 75 41 Ho4dpMCp VkmMQpuA
0150  3d 3d 22 7d =="}
    
```

Gambar 5. Lalu Lintas Data Sesudah Enkripsi

Pada Gambar 4 dan Gambar 5 terlihat perbandingan nilai dari data sebelum dan sesudah dienkripsi di software Wireshark. Hal ini menandakan bahwa hasil perbandingan sebelum dan sesudah dienkripsi, data yang belum dienkripsi bisa dibaca oleh pihak lain yang ingin mencuri data. Sedangkan data sesudah dienkripsi akan sulit untuk dibaca datanya karna perlu didekripsi terlebih dahulu.

3.3. Hasil Pengujian Fungsionalitas Aplikasi Android

3.3.1 QR Code

Tabel 2. Jarak Terjauh QR Code

Jarak Pemindaian	Status
1 cm	Terdeteksi
5 cm	Terdeteksi
10 cm	Terdeteksi
15 cm	Terdeteksi
20 cm	Terdeteksi

3.3.2 Black Box Testing

Hasil pengujian Black Box Testing pada fungsi dan fitur di aplikasi android telah memenuhi ekspektasi dengan presentase keberhasilan program 100%.

4. Kesimpulan

1. Penelitian tugas akhir mengimplementasikan aplikasi android yang mampu mengumpulkan data berat badan, suhu tubuh dan sinyal detak jantung dari IoT healthcare device dan datanya disimpan di MongoDB melalui cloud server.
2. Waktu Enkripsi dan Dekripsi data kesehatan pengguna dengan AES-256 bit pada aplikasi android berhasil dilakukan dengan rata-rata waktu 1 ms untuk kedua proses tersebut.
3. Hasil pengukuran Quality of Service dari aplikasi android ke cloud server memiliki delay rata-rata 203 ms, throughput 4.624 Kbps, dan packet loss 0% dengan metode POST dengan delay rata-rata 245 ms, throughput 9.584 Kbps, dan packet loss 0% untuk metode GET. Sedangkan hasil pengukuran Quality of Service dari perangkat IoT ke aplikasi android memiliki delay rata-rata 85 ms, throughput 2.128 Kbps, dan packet loss 0% untuk metode Notification dengan delay rata-rata 97 ms, throughput 2.424 Kbps, dan packet loss 0% untuk metode Write.
4. Menghubungkan antara aplikasi dan tiga perangkat menggunakan metode otentikasi Quick Response Code dengan jarak terjauh 20 cm dan terdeteksi oleh beberapa model ponsel dengan OS Android.
5. Fungsionalitas aplikasi android dengan metode pengujian black box telah memenuhi hasil yang diharapkan dengan persentase 100% dari hasil aktual.

Referensi:

- [1] C. Wang, "To Cope with a New Coronavirus Pandemic: How Life May Be Changed Forever," *Chinese J. Int. Law*, vol. 19, no. 2, pp. 221–228, Jun. 2020, doi: 10.1093/chinesejil/jmaa020.
- [2] "Complimentary Report Q120 | OpenVault." <https://openvault.com/complimentary-report-q120/> (accessed Oct. 13, 2020).
- [3] R. J. Rohrich, K. L. Hamilton, Y. Avashia, and I. Savetsky, "The COVID-19 Pandemic," *Plast. Reconstr. Surg. - Glob. Open*, vol. 8, no. 4, p. e2854, Apr. 2020, doi: 10.1097/GOX.0000000000002854.
- [4] "Mengenal Telemedicine Beserta Kelebihan dan Kekurangannya - Tirto.ID." <https://tirto.id/mengenal-telemedicine-beserta-kelebihan-dan-kekurangannya-fsnL> (accessed Oct. 13, 2020).

- [5] A. Giorgio, "Innovative Medical Devices for Telemedicine Applications," in *Telemedicine Techniques and Applications*, InTech, 2011.
- [6] S. Ryu, "Telemedicine: Opportunities and Developments in Member States: Report on the Second Global Survey on eHealth 2009 (Global Observatory for eHealth Series, Volume 2)," *Healthcare Informatics Research*, vol. 18, no. 2, pp. 153–155, jun 2012. [Online]. Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3402558/>
- [7] "What is IoT (Internet of Things)? — IoT Architecture & Application — Edureka." [Online]. Available: <https://www.edureka.co/blog/what-is-iot/>
- [8] "Medical Check Up, Ini yang Harus Anda Ketahui - Alodokter." [Online]. Available: <https://www.alodokter.com/medical-check-up-ini-yang-harus-anda-ketahui>.
- [9] W. Danielsson, "React native application development," *Linkopings universitet, Swedia*, vol. 10, p. 4, 2016.
- [10] "Android Overview — Open Handset Alliance." [Online]. Available: http://www.openhandsetalliance.com/android_overview.html
- [11] M. Collotta and G. Pau, "A solution based on bluetooth low energy for smart home energy management," *Energies*, vol. 8, no. 10, p. 11916–11938, Oct 2015. [Online]. Available: <http://dx.doi.org/10.3390/en81011916>
- [12] "Bluetooth Low Energy (BLE) Introduction - Part 1 — EmbeTronicX." [Online]. Available: <https://embetronicx.com/tutorials/techf gdevices/ bluetooth-low-energy-ble-introduction-part-1/>
- [13] T. Cata, P. Patel, and T. Sakaguchi, "Qr code: A new opportunity for effective mobile marketing," 2013.
- [14] K. H. Pandya and H. Galiyawala, "A survey on qr codes: in context of research and application," 2014.
- [15] S. Frankel, R. Glenn, and S. Kelly, *RFC3602: The AES-CBC Cipher Algorithm and Its Use with IPsec*. USA: RFC Editor, 2003.